



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/851,474	05/08/2001	Timofei Kouzminov	56234-077 (GUZL-152)	3785

7590 11/18/2004

McDermott, Will & Emery
28 State Street
Boston, MA 02109

EXAMINER

DAVIS, ZACHARY A

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 11/18/2004

5

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/851,474	KOUZMINOV, TIMOFEI
	Examiner	Art Unit
	Zachary A Davis	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 08 May 2001.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-15 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-15 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ . |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>3</u> . | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 2-4, 7-9, and 13-15 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Specifically, Claims 2, 7, and 13 recite that two encryptions are to take place before a decryption. Claims 3, 10, and 14 make clear that it is only one decryption that takes place after the two encryptions. The specification states that "any type of encryption algorithm may be used" as long as the algorithm adheres to the equation recited in Claims 3, 10, and 14 where an original plaintext is recovered after the three operations (see page 11 of Applicant's specification); however, encryption algorithms generally require one decryption operation to correspond to each encryption operation. Thus, it is unclear how one would use such an algorithm to recover a plaintext with two encryptions but only one decryption. The claims are therefore not sufficiently enabled by the disclosure.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1, 5, 6, and 10-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessner, "Copy Protection for SRAM based FPGA designs", in view of Eskicioglu, PCT Publication WO99/30499.

In reference to Claim 1, Kessner discloses a system for copy protecting an FPGA including a CPLD that includes a sequence generator and an FPGA that includes a sequence generator and a sequence comparison device. Kessner further discloses that the CPLD initializes its sequence generator, which generates a first sequence based on its initial value, and transmits the first sequence to the FPGA. Kessner also discloses that the FPGA initializes its sequence generator, which generates a second sequence based on its same initial value, and compares the received first sequence with the generated second sequence, and enables operation of the FPGA if the sequences match (see page 2, section "Overview"). However, Kessner does not explicitly disclose how the initial value of the sequence generators is generated; specifically, Kessner does not disclose that an initial state is generated and encrypted in the CPLD, transmitted to the FPGA, and decrypted in the FPGA.

Eskicioglu discloses a method for protecting data that includes generating an initial value (page 6, lines 18-20, where the key is the initial value, as stated at page 6, lines 11-12) and encrypting and sending the initial value to a receiver (page 6, lines 24-31). Eskicioglu further discloses that the received initial value is decrypted (page 6, lines 31-33) and that the initial value is used as a seed to generate a sequence in both the transmitter and the receiver (page 3, lines 16-32, and Figure 2, where the keystream is the generated sequence). Eskicioglu also discloses the use of a challenge sequence provided to the sequence generators (page 7, line 5-page 8, line 31, where additional inputs are used in generating the keystream sequences).

Therefore, it would have been obvious to one of ordinary skill in the art to modify the system of Kessner by sending an encrypted initial value, decrypting the received initial value, and using the decrypted initial value in generating the sequences, in order to implement renewable security to allow for the development of systems that can be replaced or upgraded more easily and with less expense (see Eskicioglu, page 1, lines 28-30).

Claims 5 and 6 contain all the limitations of Claim 1, and are therefore rejected by a similar rationale.

Claims 10 and 11 are method claims corresponding substantially to the systems of Claims 5 and 6, respectively, and are rejected by a similar rationale.

In reference to Claim 12, Eskicioglu further discloses encrypting the initial state with a key (page 6, lines 24-31).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.
 - a. McAdam et al, US Patent 4964162, discloses an encoding system in which an identifier is sent encrypted between a transmitter and a receiver, and a random seed is used to synchronize pseudorandom generators in the transmitter and receiver.
 - b. Aucsmith, US Patent 5754658, discloses an encryption process in which keys are generated from a pair of random generators that are synchronized using a securely sent seed value.
 - c. Kelem et al, US Patent 6118869, discloses a system for programmable logic device bitstream encryption.
 - d. Kobayashi, US Patent 6304100, discloses a system for copy protection of an FPGA.
 - e. Burnham, US Patent 6305005, discloses a method to configure an FPGA using encrypted macros.
 - f. Batinic et al, US Patent 6351814, discloses a system for copy protection of an encrypted FPGA program.

- g. Moskowitz, US Patent 6598162, discloses that a block cipher, seeded by a random value, can be used as a cryptographically secure random generator.
- h. Trimberger, US Patent 6654889, discloses a method for programming a programmable logic device using encrypted configuration data and verification of a hash function.
- i. Kean, US Patent Application Publication 2001/0015919, discloses a method for encrypting configuration data on an FPGA.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Matthew A. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD
zad